

NATIONAL ASSOCIATION OF ATTORNEYS GENERAL
750 FIRST STREET NE SUITE 1100
WASHINGTON, D.C. 20002
(202) 326-6019
(202) 408-6998
<http://www.naag.org>

LYNNE M. ROSS
Executive Director

PRESIDENT
STEPHEN CARTER
Attorney General of Indiana

PRESIDENT-ELECT
THURBERT BAKER
Attorney General of Georgia

VICE PRESIDENT
LAWRENCE WASDEN
Attorney General of Idaho

IMMEDIATE PAST PRESIDENT
WILLIAM H. SORRELL
Attorney General of Vermont

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

RE: CC Docket No. 96-115

Dear Ms. Dortch:

Attached please find Comments signed by 48 Attorneys General to be filed in the above-referenced proceeding regarding the privacy protections of customer proprietary network information. If you have questions about the Comments, please do not hesitate to contact Deborah Hagan, Consumer Protection Division Chief, Illinois, at (217) 782-9021; Elizabeth Blackston, Consumer Protection Bureau Chief, Illinois, at (217) 782-9021; or Esther Chavez, Texas Assistant Attorney General, at (512) 475-4628.

Thank you for your attention to this matter.

Sincerely,

/s/

Dennis P. Cuevas
Consumer Protection Counsel

Attachment

NAAG Comments – Docket No. 96-115

**Before The
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of:)
)
Implementation of the Telecommunications)
Act of 1996:)
)
Telecommunications Carriers' Use of)
Customer Proprietary Network Information)
and other Customer Information;)
)
Petition for Rulemaking to Enhance Security)
and Authentication Standards for Access to)
Customer Proprietary Network Information)
)
)

CC Docket No. 96-115

RM-11277

**COMMENTS OF
ATTORNEYS GENERAL
OF THE
UNDERSIGNED STATES**

April 28, 2006

Table of Contents

| | | |
|------|--|----|
| I. | Introduction | 1 |
| II. | Are enhanced security and authentication standards for access to customer telephone records warranted? What is the nature and scope of the problem? | 2 |
| III. | Does the existing opt out regime sufficiently protect the privacy of CPNI in the context of CPNI disclosed to telecommunications carriers' joint venture partners and independent contractors and would this change in the Commission's regulations better protect customer privacy notwithstanding the Commission's current safeguards applicable to the release of CPNI to carriers' partners and independent contractors?.. | 5 |
| IV. | Are the notices carriers provide subscribers regarding the use and disclosure of CPNI written clearly enough so that customers adequately understand that the notices concern the privacy of personal telephone records?. | 9 |
| V. | Should any requirements the FCC adopts in the context of this rulemaking extend to VoIP service providers or other IP enabled services? | 11 |
| VI. | Does the mobile and personal nature of wireless phones increase the privacy expectations of wireless customers and should wireless CPNI receive additional protection?. | 12 |
| VII. | As a general matter, are the FCC's existing regulations adequate to protect the privacy of CPNI? | 14 |

I. Introduction

On March 15, 2006, the Federal Communications Commission (FCC) published its Notice of Proposed Rulemaking (NPRM) which addresses the widely publicized privacy concerns generated by data brokers' obtaining and selling Customer Proprietary Network Information (CPNI) - sensitive personal information that includes logs of calls made and received by telephone customers.¹

Procedurally, this NPRM is in response to a petition filed by the Electronic Privacy Information Center (EPIC) in which EPIC asked the FCC to initiate a rulemaking proceeding to establish more stringent security standards for telecommunications carriers' maintenance and release of CPNI.

This NPRM also reflects the efforts of the FCC to address, along with other regulators, law makers, and law enforcement challenges presented by consumer privacy in the 21st century. Developments of the last year more clearly than ever demonstrated that the personal information of consumers is a valuable commodity. Included in the headlines were report after report of identity theft and security breaches.² Lawmakers around the country have begun to recognize the compelling need for laws which attempt to combat this scourge by imposing requirements on businesses to safeguard customer information, to notify consumers when their information has been compromised and to enable consumers to take affirmative steps to prevent unlawful use of their compromised information by thieves. At least twenty-five states now have laws which require companies to safeguard consumers' personal information and to notify consumers when their personal information has been compromised.³ At least sixteen

¹ RM-11277 relating to Telecommunications Carriers Use of Customer Proprietary Network Information (CPNI), CC Docket No. 96-115. (FCC NPRM).

² See http://www.usatoday.com/tech/news/computersecurity/2005-12-28-computer-security_x.htm. See also: A chronology of data breaches reported since February 2005, Privacy Rights Clearinghouse <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

³ Conference of Western Attorney Generals, *Comparison of Security Breach Laws*, 2006 CWAG ID Theft Summit, April 10-11, 2006.

states now have laws which permit consumers to place a freeze on their credit report to prevent unauthorized access to their credit report.⁴

Identity theft is also being battled on the enforcement front at the federal⁵ and state level. On an issue specific to this proceeding, the sale of call detail records by web site based data brokers, the States of Florida, Missouri, Illinois, California and Texas are currently engaged in litigation against brokers based in Florida, Missouri, Colorado and Utah. Other confidential investigations remain underway.

Against this backdrop, the States appreciate the Commission's moving forward to address the privacy concerns impacted by the sale and use of CPNI and appreciate the thoroughness of the series of detailed questions posed by the Commission. In these Comments, the States address those issues to which the Attorneys General, as the chief law enforcement officers of their respective states, are uniquely qualified to respond.⁶

II. Are enhanced security and authentication standards for access to customer telephone records warranted? What is the nature and scope of the problem?

The States submit that the practice of selling consumers' personal telephone information is widespread and poses a significant privacy and security risk for individual consumers as well as law enforcement.

⁴ Conference of Western Attorney Generals, *State Security Freeze Laws*, 2006 CWAG ID Theft Summit, April 10-11, 2006.

⁵ In the Matter of CardSystems Solutions, Inc., and Solidus Networks, Inc., d/b/a Pay by Touch Solutions, File No. 052 3148; United States of America (for the Federal Trade Commission) v. Choicepoint, Inc. FTC File No. 052-3069; In the Matter of DSW Inc. File No. 052 3096; In the Matter of Superior Mortgage Corp. File No. 052 3136; In the Matter of AT&T, Inc., File No. EB-06-TC-059; In the Matter of Alltel Corp., File No. EB-06-TC-058; Citation sent to LocateCell.com, File No. EB-05-TC-059; and Citation sent to Data Find.org, File No. EB-05-TC-066.

⁶ The States may, if needed, file Reply Comments addressing other issues once they have had an opportunity to review information provided by carriers in response to this NPRM.

The EPIC petition referenced 40 web sites offering to sell CPNI. The States are aware of at least 17 civil law suits which have been filed seeking to enjoin this specific sales practice.⁷

In conducting investigations and filing enforcement actions, the States verified that in fact, the sale of CPNI over the Internet has become widespread. The States further obtained information confirming at least two principal ways that data brokers acquire CPNI information: "pretexting" and unauthorized access to customer accounts on the internet. "Pretexting" is the practice of calling a carrier and pretending to have the authority to access protected records. In the pretext scenario, a data broker calls a carrier's customer service line, provides easily available information about the customer they are claiming to be in order to confirm identity and obtain requested information. If the data brokers run into an uncooperative agent, he or she simply continues to call until he or she finds a cooperative one. In some cases, the callers pose as an employee of the carrier's fraud department. In the second scenario, data brokers access the carriers' website and are able to assess what information is needed to access a customer account online or what information is needed to establish online access to the account if the customer whose records they seek has not already done so. Data brokers, some of whom subscribe to other data broker services then obtain the information required (e.g. billing address, social security number or a portion thereof, etc...), return to the carrier's website and access the customer's CPNI.

Regardless of the specific means being used by data brokers to obtain CPNI information, the fact that they advertise that this type of information can be obtained in a matter of hours and the relatively low prices at which they sell this information suggest that it does not

⁷ Cingular Wireless LLC v. Data find Solutions, Inc., et al; Cingular Wireless LL v. eFindOutTheTruth.com et al; Cingular Wireless LLC v. Get A Grip Consulting, Inc., et al; T-Mobile USA, Inc. v. 1st Source Information Specialists, Inc., et al; T-Mobile USA, Inc. v. C.F. Anderson, PI et al; Sprint Nextel Corporation d/b/a Sprint Nextel v. 1st Source Information Specialists, Inc.; Sprint Nextel Corporation d/b/a Sprint Nextel v. All Star Investigations, Inc., et al; Sprint Nextel Corporation d/b/a Sprint Nextel v. San Marco & Associates; Cellco Partnership d/b/a Verizon Wireless v. Source Resources et al.; State of Illinois v. 1st Source Information Specialists, Inc., et al.; State of Illinois v. Data Trace USA, Inc., et al; State of California v. Data Trace USA, Inc., et al.; State of Florida v. 1st Source Information Specialists, Inc., et al.; State of Florida v. Global Information Group, Inc., et al.; State of Missouri v. Data Find Solutions, Inc., et al; State of Missouri v. Data Trace USA, Inc., et al; and State of Texas v. John Strange et al.

take a significant investment of time or money for them to access CPNI. For example, the data brokers which were the subject of States' litigation offered to sell CPNI at prices ranging from \$89.95 to \$185.00.

In the States' investigations of various data brokers, the States concluded that many carriers, in their efforts to serve their customers by providing them access to their own information, had systems in place which brokers and their agents were able to exploit to obtain customer information to which they are not entitled. The carriers' systems seem to have been established before there was widespread recognition of identity theft and security breach concerns.⁸

There can be little question that the practices of the data broker industry pose significant privacy and security risks for individual telecommunications customers. Phone call records can be utilized to track a customer's communications with specific persons, businesses and medical providers. Cell phone records can also include location tracking, enabling a stalker or unscrupulous repossession company to track the whereabouts of their subject.⁹ The sale of phone records also poses threats to businesses whose records could reflect contact information for clients, provide evidence of meetings planned, hotel reservations, staff personal telephone numbers and consultation with attorneys. Call records of attorneys' offices could reflect confidential communications such as contact information for witnesses and experts while call records of physician's offices would yield patient lists.

Finally, the sale of phone records poses a serious threat to law enforcement officials by potentially compromising law enforcement work. In January, 2006, an Illinois city police official, who did not disclose his position as a police official, purchased the call records for one of the police department's wireless telephones assigned to that police department's undercover narcotics unit. With no questions asked, he was able to obtain the last 100 calls made from the

⁸ The States are reluctant to spell out specific details here out of concern that such information would serve to inspire more breaches of consumer privacy.

⁹ See *Remsburg v. Docusearch*, 149 N.H. 148, 816 A.2d 1001 (2003).

phone in only three hours.¹⁰ Criminals can use such records to expose a government informant or undercover officer who regularly calls law enforcement officials.

III. Does the existing opt out regime sufficiently protect the privacy of CPNI in the context of CPNI disclosed to telecommunications carriers' joint venture partners and independent contractors and would this change in the Commission's regulations better protect customer privacy notwithstanding the Commission's current safeguards applicable to the release of CPNI to carriers' partners and independent contractors?¹¹

The States urge the Commission to protect the privacy rights of consumers by implementing an "opt in" approach, that is, the carrier must have the affirmative express consent of a consumer before using, disclosing or permitting access to the consumer's personal telephone records. The States further urge the Commission to act decisively to bolster the existing "safeguard" rules¹² which require that the carrier and its contractor/partner have an agreement with "appropriate protections...to ensure the ongoing confidentiality of consumers' CPNI."¹³

Since its 2002 CPNI Order, the Commission rules, in relevant part, have provided that a consumer's "opt out approval" is sufficient to permit a carrier to disclose the consumer's personal telephone information outside of the carrier's company to agents, affiliates, joint venture partners and independent contractors that provide telecommunications services for the purpose of marketing telecommunications services. "Opt out" approval is also permitted as the basis for a carrier using a consumer's CPNI to market a service to a customer that the customer does not already purchase (i.e. to market wireless services to a wireline customer).¹⁴

¹⁰ People of the State of Illinois v. 1st Source Information Specialists, *et al*, filed January 20, 2006 in Sangamon County Circuit Court, Illinois (2006-CH-29).

¹¹ FCC NPRM at 7, *Supra* note 1.

¹² 47 C.F.R. § 64.2007(b)(2)(iii).

¹³ 47 C.F.R. § 64.2007(b)(2)(iii).

¹⁴ 47 C.F.R. § 64.2007.

Whereas “opt in” approval refers to a method for obtaining the consumer’s consent which requires that the carrier obtain affirmative express consent from that consumer, “opt out” means that a carrier may assume it has a consumer’s approval to share and use a consumer’s personal telephone information for marketing if the consumer does not, within 30 days after receiving notice, tell the carrier that it does NOT have approval.¹⁵ This “opt out” type of “approval” is not consistent with the ordinary meaning of the word “approval” defined as “[t]he act of confirming, ratifying, assenting, sanctioning, or consenting to some act or thing done by another. “Approval” implies knowledge and exercise of discretion after knowledge.”¹⁶

Studies conducted of “opt out” consent required under the Gramm-Leach-Bliley Act¹⁷ (GLB) demonstrate that consumers’ failure to respond does not indicate “knowledge and exercise of discretion after knowledge.” These studies demonstrated that consumers either never saw or did not understand these notices¹⁸ and that lack of time or interest and difficulty in understanding or reading the notices topped the list of the reasons why consumers did not spend more time reading those notices.¹⁹

These studies serve as confirmation of what common sense tells us: that in this harried country of multitaskers, most consumers are unlikely to read the extra notices that arrived in today’s or last week’s mail and thus, will not understand that failure to act will be treated as an affirmative consent to share his or her information.

¹⁵ See <http://www.fcc.gov/cgb/consumerfacts/phoneaboutyou.html>. FCC Consumer Advisory: *Protecting the Privacy of Your Telephone Calling Records*. Last reviewed/updated on 3/02/06.

¹⁶ BLACK’S LAW DICTIONARY 102 (6th ed. 1990).

¹⁷ Under the Gramm-Leach-Bliley Act, 15 U.S.C § 6801 et seq., banks, insurance agencies and brokerage firms were required to send notice reflecting an opportunity to “opt-out” to customers before sharing their non-public information with certain entities.

¹⁸ See Report prepared by Kleimann Communication Group: *Evolution of a Prototype Financial Privacy Notice, A Report on the Form Development Project* (February 28, 2006).

¹⁹ Harris Interactive, Inc., *Privacy Leadership Initiative: Privacy Notices Research Final Results*, Study No. 15338 (Dec. 2001). Total Respondents: 2,053 adults who are U.S. Residents, age 18 and over. Interviewing conducted online between November 9-14, 2001.

Thus, the States submit that allowing the use of an “opt out” mechanism assures that the private personal call information of a majority of customers will be widely distributed putting those customers at greater risk of identity theft and its accompanying harm.²⁰

One of the assumptions underlying this opt out regime appears to be that the relationship between the provider and the affiliate, joint venture partner or contractor provides some assurance to the customer that their information is still somehow under the control of the carrier and thus, will remain secure. And, as noted above, the current rules include a provision requiring certain joint venture/contractor safeguards.²¹ The safeguards include the requirement of an agreement between the carrier and the contractor/partner requiring that the contractor/partner have “appropriate protections in place to ensure the ongoing confidentiality of consumers’ CPNI,”²² requiring the use of CPNI only for marketing or providing the communications-related services for which the CPNI has been provided²³ and disallowing the contractor/joint venture partner from using, allowing access to, or disclosing the CPNI to any other party, unless required under force of law.²⁴

Realistically, once that CPNI information leaves a carrier, the carrier loses effective control of it. The challenges of maintaining control of personal information are evidenced by the fact that, since February of 2005, over 152 major security breaches compromising the personal identifying information and financial information of over 54 million Americans have been

²⁰ The States recognize that in 1999 the Tenth Circuit in *U.S. West, Inc. v. F.C.C.* rejected an FCC regime requiring “opt in” consent as an impermissible regulation of commercial speech. However, the Court did not hold that an opt in approach would necessarily violate the First Amendment, nor that an opt out approach was the only mechanism available that satisfied the requirements of the Constitution. Rather, the Court held that the record failed to demonstrate that (1) CPNI regulations directly and materially advance the Commission’s interest in protecting consumer privacy; and (2) that the “opt in” mechanism was sufficiently narrowly tailored. At that time, the Court observed that the government failed to show that harm to privacy was real and further reasoned that “there was no indication that disclosure of CPNI might actually occur.” 182 F.3d 1224 and 1238-1240.

²¹ 47 C.F.R. § 64.2007(b)(2).

²² 47 C.F.R. § 64.2007 (b)(2)(iii).

²³ 47 C.F.R. § 64.2007 (b)(2)(i).

²⁴ 47 C.F.R. § 64.2007 (b)(2)(ii).

reported.²⁵ Breaches were attributed to a wide variety of causes including hacking, mail theft, dishonest insiders, stolen hard drives, passwords being compromised, the establishment of bogus accounts by identity thieves to obtain access to information, lost backup tapes, stolen laptops, unintended online exposure, lost CDs, lost file boxes, and errors in distribution.²⁶ Indeed such breaches may be one of the links in the chain that results in data brokers having the personal information needed to acquire private telephone records.

CPNI information in the hands of agents, independent contractors, affiliates and joint venturers is equally vulnerable to these types of breaches. Further, in our global economy it is increasingly common for companies to shift their telemarketing services and call centers to offshore locations. The Nelson Hall research firm reports that nearly 60% of work done offshore is in customer services, including telemarketing and basic customer care functions such as order taking.²⁷ Further, Voice Over Internet Technology is predicted to reduce annual phone bills for call centers by up to 40% making the cost savings of outsourcing offshore even more attractive to U.S. based companies.²⁸

Before a consumer's personal information is shared with an untold number of entities and goes traveling around the world, a consumer should be given the opportunity to consent to expose his information to that risk. An example of legislation that uses the opt in mechanism for privacy protection is the Driver's Privacy Protection Act of 1994²⁹ which since 1999 has imposed an opt in requirement on state departments of motor vehicles before they may disclose or sell drivers' information for marketing purposes.

Further, the States would suggest that if the FCC deems it appropriate to continue to treat "opt out" as consent, it should strengthen and elaborate upon the safeguard rule which as

²⁵ A chronology of data breaches reported since the ChoicePoint incident, privacy rights clearinghouse <http://www.privacyrights.org/ar/ChronDataBreaches.htm>. Initially, these breaches are being publicized because of new states' law, beginning with California's which was implemented in July 2003 requiring entities to report data breaches to affected individuals. 22 other states now have similar security breach notification requirements. <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

²⁶ *Id* at <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

²⁷ <http://www.openoutsourcing.com/resource-dated3359-Philippines>, last reviewed April 4, 2006.

²⁸ <http://outsourcingsage.com> last reviewed April 3, 2006.

²⁹ Driver's Privacy Protection Act of 1994, (DPPA), 18 U.S.C. §§ 2721-2725.

currently written provides little guidance to carriers beyond requiring them to have an agreement that mandates CPNI will be safeguarded. For example, the rule fails to mandate audit or record keeping procedures that would facilitate review of compliance and consequent enforcement for noncompliance. Similarly, it is silent regarding whether these independent contractors, agents, affiliates and partners must return or destroy CPNI information to the carrier after they have utilized the information for the approved marketing purpose.

IV. Are the notices carriers provide subscribers regarding the use and disclosure of CPNI written clearly enough so that customers adequately understand that the notices concern the privacy of personal telephone records?³⁰

In considering the Commission's request for comments on this issue, the States reviewed the CPNI policies as posted at the web sites of major carriers. While acknowledging the efforts of the carriers in posting information at their respective web sites, the States submit that the language, choice of words and format in which this information is provided creates consumer confusion which results in consumers not being able to exercise the control over CPNI which Congress intended.

These notices generally reflect a dense language style including use of words whose meaning is not explained at the web site. For example, if a carrier represents that it will not disclose CPNI without your consent except to "business partners," does this literally mean that they share this information only with persons and entities with whom they have established a partnership under the law or are they referring to some other definition of partnership? Similarly, it is not clear what carriers really mean when they refer to sharing information with "affiliates" and consumers cannot be expected to understand what the carriers mean when they use regulatory phrases like "call detail records."

Further, each of the carriers' explanations of their respective CPNI policies and practices are so dissimilar that a consumer whose choice of provider might be affected by such policies would not be able to compare policies on the basis of these explanations. While many of the carriers literally incorporate the language of the federal regulation which provides the customer "has a right and the carrier has a duty under the law, to ensure the confidentiality of

³⁰ See FCC NPRM at 11, *Supra* note 1.

CPNI” the very definition of what CPNI exactly is varies from carrier to carrier. As the Commission notes in its NPRM, “CPNI is not a term with which most customers are familiar.”³¹

Further, the carriers’ web sites too often include statements such as “Carrier will not disclose your CPNI except as allowed by law” and precisely what is allowed by law is not made clear. These types of statements result in the sentence having no real meaning to consumers and contribute to consumer confusion.

Moreover, some carriers’ sites provide information regarding what specific steps a customer must take to opt-out of receiving unsolicited e-mail, faxes, phone calls and text messages, but omit any specific information or instructions explaining how a customer can exercise his or her CPNI related right to “opt out.” Some web sites refer to how they will not utilize CPNI without obtaining customer “approval” and do not clearly explain the circumstances in which “approval” requires no affirmative act on the part of the consumer but rather is assumed.

The States would ask the FCC to protect consumer privacy rights regarding CPNI notices by requiring carriers to issue uniform, standard notices in a brief format and to develop the new notice requirement based on scientific expertise.³² Absent these changes, the States do not believe that Congressional intent regarding giving consumers the opportunity to control how their CPNI will be used and with whom it will be shared will be implemented.

The States position is based upon their experience in the enforcement of consumer protection laws, many of which deal with issues regarding whether or not consumers were misled or confused by representations, including disclosures made by a company.

The States recommend that the FCC consider adoption of a short form notice which will include a format and concise, plain language explanations of the types of information shared, what specific steps a consumer must take to exercise his or her opt out or opt in right (including relevant contact information such as web site and mailing addresses). To assure readability, the

³¹ See FCC NPRM, *Supra* note 1.

³² Extensive research has been conducted on how consumers learn from notices. See, e.g., Manoj Hastak Ph.D., The Effectiveness of “Opt-Out” Disclosures in Pre-Screened Credit Card Offers,” submitted to the FTC September 2004; and Bettman, J.R., Payne, J.W., and Staelin, R. (1986). Cognitive Considerations in Designing Effective Labels for Presenting Risk Information. *Journal of Public Policy and Marketing*, 5, 1-28.

Commission should also provide standards for text font, size and background applicable to the means by which the notice is communicated (e.g. written as opposed to electronic notices). The States also recommend that the Commission consider adopting a requirement that all carriers which maintain web sites post their current CPNI notices in a format to be provided by the Commission.

V. Should any requirements the FCC adopts in the context of this rulemaking extend to VoIP service providers or other IP enabled services?

Providers of VoIP services generally have not been burdened with the same regulatory obligations imposed upon traditional providers of circuit-switched telecommunications services. This has enabled certain services, such as e-mail and Internet access providers, which have been classified as “information services” to flourish free from the obligations imposed by telecommunication service regulations. IP-enabled service providers have contended that their services should also fall into the category of “information services” as opposed to “telecommunications services.”³³

The NPRM asks for comment on the subject: “Should any requirements the Commission adopts in the context of the present rulemaking extend to VoIP service providers or other IP enabled service providers?”³⁴

The States assert that in the context of VoIP enabled telephone service, the same types of records of calls received and made are maintained by providers and as such, VoIP consumers have the same privacy concerns as consumers who utilize wireline or wireless services. Thus, the States urge that the regulatory structure must provide the same level of privacy to these consumers. Allowing a lesser standard of privacy for VoIP consumers will ultimately put VoIP providers at a competitive disadvantage.

³³ Cherie R. Kiser, *Cable Television Law 2006: Competition in Video, Internet & Telephony, Faster...Easier...Cheaper...Can Regulators Keep up with the Thriving Market for Cable Provided VoIP Services?* 854 PLI/Pat 429, page 3 (2006).

³⁴ See FCC NPRM at 12, *Supra* note 1.

VI. Does the mobile and personal nature of wireless phones increase the privacy expectations of wireless customers and should wireless CPNI receive additional protection?³⁵

In addition to requiring carriers to obtain a consumer's express consent before using or sharing CPNI for marketing purposes, the FCC should require carriers to obtain express authorization prior to disclosure or sharing of a consumer's location information.

Since 1998, the FCC has required wireless communications providers to begin equipping their phones and systems with the technology needed to locate and transmit the location of a cell phone user to a public safety answering point (PSAP) so that emergency responders can respond to 911 calls made on wireless telephones.³⁶ Implementation of this requirement means in part that location information for cell phone customers is readily available.

There can be little question that location information would have great market value for advertisers interested in targeting specific consumers on the basis of routes traveled and merchants frequented and further, that such information could be used for unlawful purposes ranging from stalking to harassing debt collection practices.

"Location" information is within the statutory definition of CPNI and in its 2002 CPNI order, the FCC established its customer consent standards for all CPNI³⁷ which, as discussed, includes "opt out" consent for marketing of communications-related services and disclosure for purpose of marketing communications-related services to agents, affiliates that provide communications-related services, and joint venture partners and independent contractors. Wireless location information, however, is also subject to protection by Section 222(f)³⁸ and the

³⁵ See FCC NPRM at 11, *Supra* note 1.

³⁶ Wireless Telecommunications Bureau Standardizes Carrier Reporting on Wireless E911 Implementation, CC Docket No. 94-102, Public Notice, 18 F.C.C.R. 11420 (WTB 2003). *See also* 47 C.F.R. §20.18.

³⁷ 47 U.S.C. § 222(h)(1) (2000).

³⁸ 47 U.S.C. § 222(f).

standard articulated in that subsection is that “express authorization” is required prior to disclosure of or access to location information. At least one commentator has suggested that Congress’ choice of words means that, with the exceptions for emergencies as referenced in Section 222(g), “clear, unmistakable customer approval is required before using or disclosing location information relating to wireless subscribers.”³⁹ In 2002, the FCC declined a request for rulemaking to establish “fair location practices” under Section 222(f) reasoning that the law provides clear protections for consumers and legal obligations for providers.⁴⁰

Lest there be any doubt regarding the type of consent which a provider must obtain under Section 222(f) and how it must be provided,⁴¹ the States would encourage the FCC to clarify that, with the exceptions made for emergencies provided for in Section 222(d)(4)⁴² location information can be used or shared only after a provider has first obtained express authorization from a customer and that under no circumstances, should “opt out” be considered express authorization.

VII. As a general matter, are the FCC’s existing regulations adequate to protect the privacy of CPNI?⁴³

Due to the apparent ease with which data brokers obtain CPNI from telecommunications carriers by pretexting or through unauthorized access to online accounts, the States do not believe current regulatory safeguards to protect CPNI privacy are adequate. The States recommend that the Commission look to the process the Federal Trade Commission (the “FTC”) has undertaken regarding privacy of financial institution customer data. Pursuant to the

³⁹ Ellen Traupman, *Who Knows Where You Are? Privacy and Wireless Services*, 10 Comm. L. Conspectus, 133, 135-135 (2001).

⁴⁰ *In Re Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices*, 17 F.C.C.R. 14832 (2002).

⁴¹ 47 U.S.C. § 222(f).

⁴² 47 U.S.C. § 222(d)(4).

⁴³ See FCC NPRM at 7, *Supra* note 1.

GLB, the FTC has enacted the Safeguards Rule.⁴⁴ The Safeguards Rule requires financial institutions to develop a written information security plan describing their program to protect customer information.

As part of this information security plan, institutions must: (1) designate one or more employees to coordinate the safeguards; (2) identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks; (3) design and implement a safeguards program, and regularly monitor and test it; (4) select appropriate service providers and contract with them to implement safeguards; and (5) evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.

The requirements are meant to be flexible. The plan must be appropriate to the institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. The Safeguards Rule stresses three areas of importance to information security: (1) employee management and training; (2) information systems; and (3) managing system failures.

Following are specific practices the States recommend that the Commission and telecommunications carriers consider when evaluating the effectiveness of carriers' security plans:

1. Does the carrier disclose billing record information through fax or email? We believe data brokers primarily obtain CPNI through requesting the records be faxed or emailed to them. By stopping the practice of faxing or emailing CPNI and only sending a hard copy through the mail to the address listed on the account, telecommunication carriers can effectively prevent these records from falling into the wrong hands. While some consumers will be inconvenienced by not having immediate access to their records, the inconvenience of a two or

⁴⁴ 16 C.F.R. § 314.1 et seq.

three day wait for the hard copy of their records to arrive is small compared to the benefit of stopping data brokers from improperly acquiring their records.

In the alternative, if customers desire to have instant access to their records via email, carriers should first send a text message to the customer's phone, to which the customer must respond in the affirmative, before the information is released to the customer via email. This verification process will greatly limit data brokers who attempt to gain access to customers' CPNI by convincing customer service representatives to send the information to an email address under the data broker's control. Even if a data broker has obtained all the necessary information about the customer to convince a customer service representative to release the information, the data broker would not be able to obtain the records unless he or she physically obtains the phone from the customer. This procedure can be used for changing passwords and setting up online accounts as well. Furthermore, if a data broker tries to obtain a customer's CPNI, the customer would immediately be alerted to this fact due to the text message received.

2. Does the carrier issue employee specific passwords to each employee? Carriers could require that this password must be disclosed before any billing information would be disclosed to that employee. Data brokers have acquired CPNI through pretexting by posing as telecommunications carrier employees. By issuing an employee specific password, and matching up that password with the name given, customer service representatives can verify the person on the other end of the phone is in fact another carrier employee, and not a data broker attempting to obtain a customer's CPNI to which they are not entitled.

3. Does the carrier issue an account password when the customer first signs a contract with the carrier and require the customer to provide the password before he or she can access his/her CPNI? Data brokers consistently demonstrate they can obtain almost any type of personal information about people including social security numbers and mother's maiden name (information which could be used to verify a customer's identity). By issuing a customer personal account password, a customer would have a way of identifying himself or herself that data brokers will not have access to. This password will also be needed to set up and access

their online account. If a customer lost this password, it would be mailed to him or her at the current address associated with the account or could be emailed to him or her at the email address associated with the account. While some oppose password authentication systems because individuals sometimes forget passwords, the States would ask the Commission to investigate various means now available to manage passwords including "shared secrets" protocols in which a consumer is asked a "shared secret" question or questions that can be asked and answered by a customer.

4. Does the carrier require every customer to show photo identification when trying to obtain a copy of his or her bill from a carrier's store? Currently, a data broker could foreseeably go into a telecommunications carrier's store and pose as a customer wishing to obtain a copy of his or her phone bill. By requiring every customer to show photo identification before supplying a copy of his or her bill, or any CPNI, carriers can ensure the person to whom the information is being disclosed is the actual customer.

5. The States also recommend that the Commission, while being mindful of cost issues which the carriers can be expected to assert, thoroughly explore implementing a requirement for audit trail systems beyond its current rules.⁴⁵ Opponents of auditing argue that there is no such thing as a perfect security system and the States agree with that assertion. Increasingly, however, the approach that security experts recommend is one which acknowledges that because no system is perfect, all systems must incorporate components such as auditing which will enable them to spot and prevent activity that indicates a potential intrusion as well as to identify the specific means and persons responsible for that intrusion.⁴⁶ Applied to the instant scenario, electronic audit trails can be used to proactively identify instances where, for example, a particular customer service representative is accessing an abnormally high number of records.

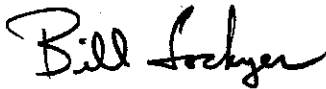
⁴⁵ 47 C.F.R. § 64.2009(c).

⁴⁶ See BRUCE SCHNEIER, *SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD* (John Wiley & Sons, 2000).

6. Does the carrier provide notice to its customer when CPNI pertaining to that customer is disclosed? Such a practice could allow the customer to object if he or she did not make a request for disclosure of CPNI. If notice is not provided, then neither the carrier nor the customer knows that his or her CPNI is being disclosed to an unauthorized person. Notice may safeguard against disclosure of CPNI to unauthorized people and may enable the unauthorized person to be identified if the unauthorized disclosure is discovered immediately.

We thank you for the opportunity to provide our views concerning this matter. If you have questions about our comments, please do not hesitate to contact Deborah Hagan, Division Chief, Consumer Protection, Illinois, (217) 782-9021 or Elizabeth Blackston, Consumer Protection Bureau Chief, Illinois, (217) 782-9021 or D. Esther Chavez, Texas Assistant Attorney General, at (512) 475-4628.

Respectfully submitted,



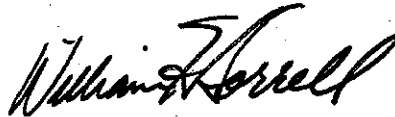
Bill Lockyer
Attorney General of California



Lisa Madigan
Attorney General of Illinois



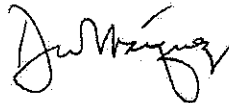
Greg Abbott
Attorney General of Texas



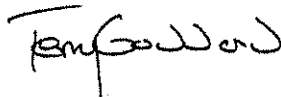
William Sorrell
Attorney General of Vermont



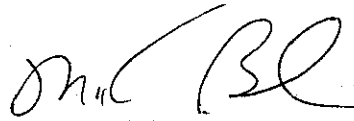
Troy King
Attorney General of Alabama



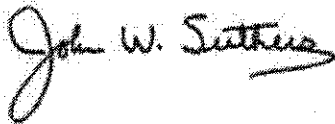
David Márquez
Attorney General of Alaska



Terry Goddard
Attorney General of Arizona



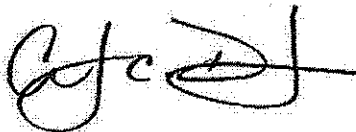
Mike Beebe
Attorney General of Arkansas



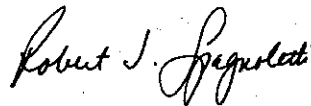
John Suthers
Attorney General of Colorado



Richard Blumenthal
Attorney General of Connecticut



Carl Danberg
Attorney General of Delaware



Robert Spagnoletti
Attorney General of District of Columbia



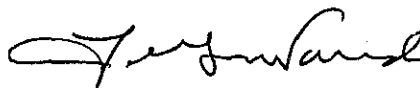
Charlie Crist
Attorney General of Florida



Thurbert Baker
Attorney General of Georgia



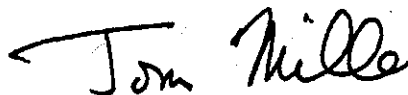
Mark Bennett
Attorney General of Hawaii



Lawrence Wasden
Attorney General of Idaho



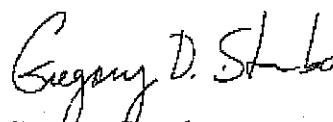
Stephen Carter
Attorney General of Indiana



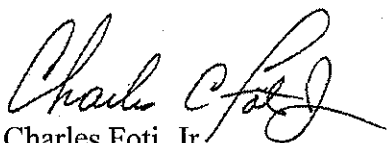
Tom Miller
Attorney General of Iowa



Phill Kline
Attorney General of Kansas



Gregory Stumbo
Attorney General of Kentucky



Charles Foti, Jr.
Attorney General of Louisiana



G. Steven Rowe
Attorney General of Maine



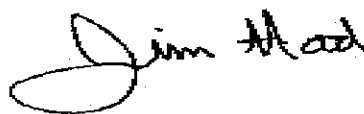
J. Joseph Curran, Jr.
Attorney General of Maryland



Tom Reilly
Attorney General of Massachusetts



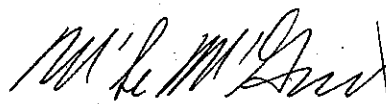
Mike Hatch
Attorney General of Minnesota



Jim Hood
Attorney General of Mississippi



Jeremiah W. Nixon
Attorney General of Missouri



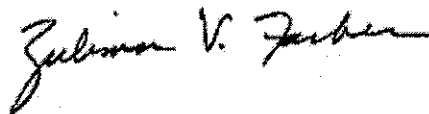
Mike McGrath
Attorney General of Montana



George Chanos
Attorney General of Nevada



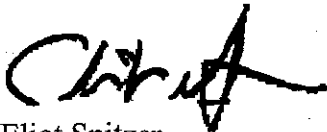
Kelly Ayotte
Attorney General of New Hampshire



Zulima Farber
Attorney General of New Jersey



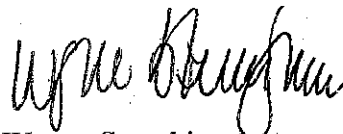
Patricia Madrid
Attorney General of New Mexico



Eliot Spitzer
Attorney General of New York



Roy Cooper
Attorney General of North Carolina



Wayne Stenehjem
Attorney General of North Dakota



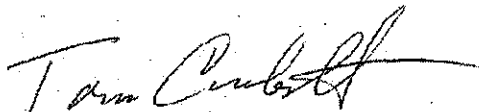
Jim Petro
Attorney General of Ohio



W.A. Drew Edmondson
Attorney General of Oklahoma



Hardy Myers
Attorney General of Oregon



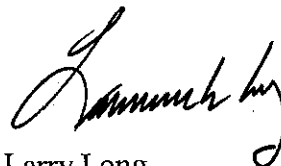
Tom Corbett
Attorney General of Pennsylvania



Patrick Lynch
Attorney General of Rhode Island



Henry McMaster
Attorney General of South Carolina



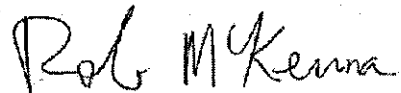
Larry Long
Attorney General of South Dakota



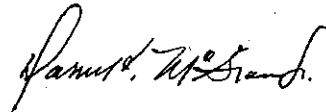
Paul Summers
Attorney General of Tennessee



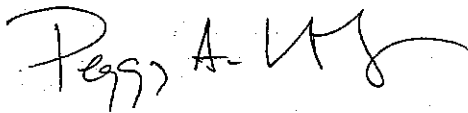
Mark Shurtleff
Attorney General of Utah



Rob McKenna
Attorney General of Washington



Darrell V. McGraw, Jr.
Attorney General of West Virginia



Peggy Lautenschlager
Attorney General of Wisconsin



Patrick Crank
Attorney General of Wyoming